Contents

Introduction

This document describes why you might encounter payload encryption and encrypted tunnel/Transport Layer Security (TLS) session limits and what to do in such a situation. Due to strong crypto export restrictions enforced by the United States government, a securityk9 license only allows payload encryption up to rates close to 90 Megabits per second (Mbps) and limits the number of encrypted tunnels/TLS sessions to the device. 85Mbps is enforced on Cisco devices.

Background Information

The crypto curtailment restriction is enforced on Cisco Integrated Service Router (ISR) series routers with the Crypto Export Restrictions Manager (CERM) implementation. With CERM implemented, before the Internet Protocol Security (IPsec)/TLS tunnel goes live, it requests CERM to reserve the tunnel. Later, IPsec sends the number of bytes to be encrypted/decrypted as parameters and queries CERM if it can proceed with encryption/decryption. CERM checks against the bandwidth that remains and responds with yes/no to process/drop the packet. Bandwidth is not reserved by IPsec at all. Based on the bandwidth that remains, for each packet, a dynamic decision is made by CERM whether to process or to drop the packet.

When IPsec must terminate the tunnel, it must free up the earlier reserved tunnels so that CERM can add them to the free pool. Without the HSEC-K9 license, this tunnel limit is set at 225 tunnels. This is shown in the output of **show platform cerm-information**:

```
router# show platform cerm-information
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED

----------------------------------------------------------------
Resource Maximum Limit Available
----------------------------------------------------------------
Tx Bandwidth(in kbps) 85000 85000
Rx Bandwidth(in kbps) 85000 85000
Number of tunnels 225 221
Number of TLS sessions 1000 1000
```

> **Note**: On the ISR 4400/ISR 4300 Series routers that run Cisco IOS-XE®, the CERM

limitations also apply, unlike on the Aggregation Services Router (ASR)1000 Series routers. They can be viewed with the output of **show platform software cerm-information**.

How are the limits calculated?

In order to understand how the tunnel limits are calculated, you must understand what a proxy identity is. If you already understand proxy identity, you can continue to the next section. The proxy identity is the term used in the context of IPsec that designates the traffic protected by an IPsec Security Association (SA). There is a one-to-one correspondence between a permit entry on a crypto access-list and a proxy identity (proxy ID for short). For instance, when you have a crypto access-list defined like this:

```
router# show platform cerm-information
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED

----------------------------------------------------------------
Resource Maximum Limit Available
----------------------------------------------------------------
Tx Bandwidth(in kbps) 85000 85000
Rx Bandwidth(in kbps) 85000 85000
Number of tunnels 225 221
Number of TLS sessions 1000 1000
```

This translates to exactly two proxy IDs. When an IPsec tunnel is active, you have a minimum of one pair of SAs negotiated with the end point. If you use multiple transforms, this could increase up to three pairs of IPsec SAs (one pair for ESP, one for AH, and one for PCP). You can see an example of this from the output of your router. Here is the **show crypto ipsec sa** output***:***

```
router# show platform cerm-information
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED

----------------------------------------------------------------
Resource Maximum Limit Available
----------------------------------------------------------------
Tx Bandwidth(in kbps) 85000 85000
Rx Bandwidth(in kbps) 85000 85000
Number of tunnels 225 221
Number of TLS sessions 1000 1000
```

Here are the IPsec SA pairs (inbound-outbound):

```
router# show platform cerm-information
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED

----------------------------------------------------------------
Resource Maximum Limit Available
----------------------------------------------------------------
Tx Bandwidth(in kbps) 85000 85000
Rx Bandwidth(in kbps) 85000 85000
Number of tunnels 225 221
Number of TLS sessions 1000 1000
```

In this case, there are exactly two pairs of SAs. These two pairs are generated as soon as traffic hits the crypto access-list that matches the proxy ID. The same proxy ID could be used for different peers.

> **Note**: When you examine the output of **show cry ipsec sa,** you see that there is a current outbound Security Parameter Index (SPI) of 0x0 for the inactive entries and an existing SPI when the tunnel is up.

In the context of CERM, the router counts the number of active proxy ID/peer pairs. This means that if you had, for example, ten peers for which you have 30 permit entries in each of the crypto access-lists, and if there is traffic that matches all of those access-lists, you end up with 300 proxy ID/peer pairs which is above the 225 limit imposed by CERM. A quick way to count the number of tunnels that CERM considers is to use the **show crypto ipsec sa count** command and look for the IPsec SA total count as shown here:

```
router#show crypto ipsec sa count
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```

The number of tunnels is then easily calculated as the total IPsec SA count divided by two.

Problem

Symptoms

These messages are seen in the syslog when the crypto curtailment limits are exceeded:

```
router#show crypto ipsec sa count
IPsec SA total: 6, active: 6, rekeying: 0, unused: 0, invalid: 0
```

Root Cause

It is not uncommon for routers to be connected via Gigabit interfaces, and as explained previously, the router starts to drop traffic when it reaches 85 Mbps inbound or outbound. Even in cases where Gigabit interfaces are not in use or the average bandwidth utilization is clearly well below this limit, transit traffic can be bursty. Even if the burst is for a few **milliseconds**, it is enough to trigger the curtailed crypto bandwidth limit. And in these situations, the traffic that exceeds 85Mbps is dropped and accounted in **show platform cerm-information** output***:***

```
router#show platform cerm-information | include pkt
Failed encrypt pkts: 42159817
Failed decrypt pkts: 0
Failed encrypt pkt bytes: 62733807696
Failed decrypt pkt bytes: 0
Passed encrypt pkts: 506123671
Passed decrypt pkts: 2452439
Passed encrypt pkt bytes: 744753142576
Passed decrypt pkt bytes: 1402795108
```

For example, if you connect a **Cisco 2911** to a **Cisco 2951** via IPsec Virtual Tunnel Interface (VTI) and deliver an average of 69 mps of traffic with a packet generator, where the traffic is delivered in bursts of **6000 packets** at a **throughput of 500 Mbps**, you see this in your syslogs:

```
router#
Apr 2 11:52:30.028: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps
reached for Crypto functionality with securityk9 technology package license.
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62930990016
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747197374528
Passed decrypt pkt bytes: 1402795108
```

```
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62931497424
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747203749120
Passed decrypt pkt bytes: 1402795108
router#
```

As you can see, the router constantly drops the bursty traffic. Note the **%CERM-4-TX_BW_LIMIT** syslog messageis rate-limited to one message per minute.

```
router#
Apr 2 11:52:30.028: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps
reached for Crypto functionality with securityk9 technology package license.
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62930990016
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747197374528
Passed decrypt pkt bytes: 1402795108
router#show platform cerm-information | include pkt
Failed encrypt pkt bytes: 62931497424
Failed decrypt pkt bytes: 0
Passed encrypt pkt bytes: 747203749120
Passed decrypt pkt bytes: 1402795108
router#
```

Troubleshoot

For Issues Where the Bandwidth CERM Limit is Reached

Complete these steps:

1. Mirror the traffic on the connected switch.
2. Use Wireshark in order to analyze the captured trace by going down to two to 10 msec time period granularity.
   Traffic with micro bursts greater than 85Mbps is an expected behavior.

For Issues Where the Maximum Tunnel CERM Limit is Reached

Collect this output periodically in order to help identify one of these three conditions:

- The number of tunnels has exceeded the CERM limit.
- There is a tunnel count leak (number of crypto tunnels as reported by crypto statistics exceeds the actual number of tunnels).
- There is a CERM count leak (number of CERM tunnel count as reported by CERM statistics exceeds the actual number of tunnels).

Here are the commands to use:

```
show crypto eli detail
show crypto isa sa count
show crypto ipsec sa count
show platform cerm-information
```

Solution

The best solution for users with a **permanent** securityk9 license that encounter this issue is to purchase the **HSEC-K9** license. For information on these licenses, refer to Cisco ISR G2 SEC and

HSEC Licensing.

Workaround

One possible workaround for those who absolutely do not need the increased bandwidth is to implement a traffic shaper on the neighboring devices on both sides in order to smooth out any traffic bursts. The queue depth might have to be tuned based on the burstiness of the traffic in order for this to be effective.

Unfortunately this workaround is not applicable in all deployment scenarios, and often does not work well with microbursts, which are traffic bursts that occur in very short time intervals.